(Allegato 5)

MISURE DI SICUREZZA DEL SISTEMA INFORMATICO

Art.1 Misure di sicurezza del sistema informatico

Al fine di individuare ed applicare adeguate misure volte a garantire la sicurezza del sistema informatico, occorre valutare sia la vulnerabilità degli elementi costitutivi l'architettura del sistema informatico sia i dati che in esso sono collocati.
A tale scopo si rilevano le seguenti minacce, a prescindere dall'origine dolosa, colposa o accidentale degli agenti che le possono generare:

- Distruzione documenti
- Perdita anche accidentale
- Accesso non consentito
- Trattamento non autorizzato

A tal fine devono essere predisposte delle misure minime di sicurezza:

- Fisiche
- Logiche
- Organizzative

Art.2 Misure fisiche

Il ruolo della sicurezza fisica è quello di proteggere i sistemi, le aree e le componenti del sistema informativo. Un'adeguata protezione dei luoghi di lavoro serve a garantire la sicurezza dei dati custoditi al loro interno.
Nel Comune di Alessandria della Rocca il server è situato in apposita sala situata al piano terra dell'edificio, le chiavi di accesso alla sala sono custodite dal responsabile di sistema.
Possono accedere ai locali: il referente informatico/amministratore di sistema, il responsabile del servizio protocollo, il segretario comunale ed il personale che deve accedervi per l'espletamento dei compiti propri per le necessità di gestione e manutenzione dei sistemi e comunque per attività indispensabili. Nessun soggetto estraneo può accedere ai sistemi server se non accompagnato dal responsabile di sistema.
Gli interventi di manutenzione o adeguamento sui server sono richiesti ed autorizzati dall'amministratore di sistema. Quando, per l'espletamento di compiti di servizio e per altre attività, è necessario consentire l'accesso a personale esterno, occorre che il locale venga aperto dal personale custode delle chiavi (amministratore di sistema) il quale al termine dell'intervento dovrà provvedere alla chiusura dei locali.
Tra gli eventi fisici che possono portare alla perdita dei dati per distruzione delle apparecchiature vengono considerati incendio, surriscaldamento delle apparecchiature, anomalie di alimentazione elettrica e altri eventi (allagamenti, crolli, ecc…).
Contro l'eventualità che un incendio nei locali in cui sono custoditi i sistemi server possa causare danni irreversibili ai dati, è stato installato in prossimità del server un dispositivo antincendio.
Contro l'eventualità che anomalie dell'alimentazione elettrica dei sistemi server possa danneggiare i dati è stato predisposto un collegamento ad un gruppo di continuità.
Inoltre la chiusura della sala server garantisce la protezione delle apparecchiature da danneggiamenti accidentali o intenzionali.
Per evitare il rischio di accesso fisico ai locali in cui vi sono uno o più postazioni di lavoro dotate di PC o l'intrusione da parte di persone non autorizzate si devono adottare le seguenti misure di sicurezza:

- Le postazioni di lavoro devono essere accessibili solo da quanti ne hanno titolo in qualità di responsabili o incaricati del trattamento, di amministratori di sistema o altro;

- Gli uffici aperti al pubblico devono essere presidiati da personale; negli orari diversi da quelle di servizio, ove non vi sia comunque un presidio, la porta di accesso all'edificio deve rimanere chiusa;
- La persona esterna può accedere solo quando è presente qualche addetto;
- Se sono necessari interventi di manutenzione sulla macchina o di assistenza, adeguamento, ecc… presso la postazione di lavoro, è necessario che l'utente o il referente informatico o, in loro assenza altro dipendente della struttura, assista alle operazioni di manutenzione. La segreteria deve trattenere e conservare copia del rapporto di intervento rilasciato dalla ditta intervenuta. Tale rapporto deve contenere data e orario dell'intervento (inizio e fine) descrizione sintetica della ditta, firma del tecnico e dell'utente che assiste all'intervento, del tipo di intervento, nome e cognome del tecnico intervenuto.

Infine al fine di ridurre al minimo i rischi di distruzione o perdita di dati è consigliabile prediligere il lavoro sui dischi di rete la cui protezione è assicurata dalle misure di sicurezza e di salvataggio automatico adottate per i server.

Art.3 Misure logiche

Per sistema di sicurezza logica s'intende la sicurezza finalizzata all'implementazione dei requisiti di sicurezza nelle apparecchiature informatiche, dotato quindi di meccanismi opportuni e di specifiche funzioni di gestione e controllo.
Ai sensi della normativa vigente. Il trattamento di dati personali effettuato con strumenti elettronici è consentito se sono adottate le seguenti specifiche tecniche:

a) Autenticazione informatica;
b) Adozione di procedure di gestione delle credenziali di autenticazione;
c) Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
d) Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

I servizi di sicurezza logica attivati sono:

- Controllo accessi
- Autenticazione
- Confidenzialità
- Integrità

I meccanismi di sicurezza utilizzati, ovvero le modalità tecniche attraverso le quali è possibile realizzare i servizi di sicurezza sono:

- Meccanismi per il controllo degli accessi
- Meccanismi per l'autenticazione
- Meccanismi di salvataggio dati
- Antivirus

Il controllo degli accessi consiste nel garantire che tutti gli accessi agli oggetti del sistema informatico avvengano esclusivamente secondo modalità prestabilite.

Autenticazione - Per garantire quanto sopra esposto il sistema informatico comunale è basato su un meccanismo che costringe ogni utente ad autenticarsi (cioè dimostrare la propria identità) prima di poter accedere ai programmi informatici comunali ed effettuare specifici trattamenti di dati. Ad

ogni utente interno del Sistema Informatico Comunale è stata assegnata una credenziale di autenticazione, un codice identificativo personale costituito da nome utente e password, che consentono l'identificazione e l'accesso al proprio elaboratore ed alle risorse di rete.

Confidenzialità – Grazie al sistema di autenticazione predetto, l'accesso ai documenti informatici ed il trattamento di dati personali con strumenti elettronici è consentito ai soli incaricati autorizzati a quello specifico trattamento.

Integrità fisica – Al fine di evitare i rischi di perdita dei dati informatici, temporanea o definitiva e consentire il recupero di dati o file accidentalmente eliminati o erroneamente modificati, ovvero non disponibili per guasti hardware e software, limitando i disagi connessi con la discontinuità del servizio, è opportuno adottare una politica di backup sia sul server sia sulle postazioni di lavoro.
Tutti i dati dei sistemi informativi comunali ed i file presenti sui server centralizzati sono interessati da una politica di backup periodico su base giornaliera con controllo dell'avvenuto salvataggio. Il controllo viene effettuato da personale preposto allo scopo. Il backup è gestito in automatico dal sistema server.

Integrità logica – L'integrità logica si ottiene con il meccanismo di verifica dei privilegi di accesso ai file, garantito dal sistema operativo e con il sistema antivirus.
Ogni utente, superata la fase di autenticazione avendo accesso ai propri dati residenti nella propria area di lavoro, non può accedere alle altre aree né agli applicativi privo di autorizzazione. I virus sono particolari programmi predisposti per essere eseguiti all'insaputa dell'utente, che possono causare danni ai dati memorizzati sul computer o al sistema operativo del computer stesso.
Sul server Windows NT2003 l'amministratore di sistema installa e provvede a mantenere un software antivirus che garantisce una protezione idonea ad evitare il verificarsi di danni ai dati causati dai virus informatici. Il sistema antivirus risiede oltre che sul server principale, sulle postazioni di lavoro utente.

Art.4 Misure organizzative

Gli aspetti organizzativi riguardano principalmente la definizione di ruoli, compiti e responsabilità per la gestione di tutte le fasi del processo di sicurezza e l'adozione di specifiche procedure che vadano a completare e rafforzare le contromisure tecnologiche adottate.

Sono già state poste in essere alcune misure, in particolare:

- Individuazione dei responsabili del trattamento dei dati personali;
- Adozione di un regolamento per la tutela della riservatezza dei dati personali (Delibera consiliare n.72 del 22/12/2006);
- Approvazione documento programmatico sulla sicurezza – Aggiornamento (Delibera Giunta Comunale n.25 del 27/03/2009);
- Nomina amministratore di sistema (determinazione sindacale n. 25 del 10/12/2009)
- Nomina responsabile della conservazione e gestione dei flussi documentali e Responsabili per la tenuta del protocollo informatico (determinazione sindacale n.8 del 29/03/2017).